REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of Claims

Claims 1-21 are pending in this application. Claims 1, 14, 15 and 16 are independent. The remaining claims depend, directly or indirectly, from claims 1 and 16. Applicant notes that the rejection of independent claim 14 is not specifically addressed in the Office Action mailed February 28, 2005.

Drawings

Applicant respectfully requests the Examiner to accept the drawings filed on June 29, 2001.

Rejections under 35 U.S.C. § 102

Claims 1, 2, 5-9, 11, 16, 17, 19, and 20 stand rejected under 35 U.S.C. 102(b) as being anticipated by Microsoft Windows NT Server ("NTS"). Independent claims 1, 15, and 16 have been amended to clarify the present invention recited. To the extent that this rejection may still apply to the amended claims, this rejection is respectfully traversed. For anticipation under 35 U.S.C. § 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present.

The claimed invention relates to computer security in the form of a smart card-based computer access system that includes logging of user activity. More specifically, the claimed invention is directed toward providing security measures for a system for home or small business use, in which smart cards are utilized to gain access to computer functions (See Specification, page 3, lines 4-6). The user is presented with a login prompt that permits login using the smart card. Additionally, the user is permitted to bypass the use of the smart card and obtain access, but such access is logged for review by an administrator. The method of the claimed invention involves receiving a request to log into the computer system and determining whether a smart card is being used as part of the login. If a smart card is being used to login, then the user

6

associated with the smart card is provided access to the computer system based on the access control restrictions *on the smart card.* Alternatively, if a smart card is not being used to login, then an unknown user is provided access to the computer, while the access is logged for review by an administrator. Advantageously, the claimed invention allows the user to log in without the smart card if need be, while still being detected by an administrator (*e.g.*, a parent wishing to monitor a child's computer access, etc.).

NTS is directed toward the security architecture and features of the Windows NT Server Operating System. Basically, NTS is a user's guide that explains how to use and what to know about the Windows NT Server Operating System. With respect to the rejection of the claims, the Examiner asserts that NTS discloses each and every limitation of independent claim 1. Applicant respectfully disagrees with this assertion. Claim 1 has been amended to include the limitation reciting that a user using a smart card is provided access based on access restrictions on the smart card itself. Support for this amendment may be found, for example, on page 8-9 of the Specification. NTS fails to disclose or suggest that a user using a smart card to login to the system is provided access based on access restrictions on the smart card. Rather, NTS discloses that users may use token devices that generate one-time passwords for login purposes. NTS is completely silent regarding access restrictions embedded on the security token.

Further, access restrictions provided on *a smart card* is **not** the same as access restrictions associated with a user that are on *the system.* For example, a user may use a security token to log into a system, where upon validation of the security token, the system imposes access restrictions based on the authentication of the user. This is not the same as embedding access restrictions on the smart card itself, where the smart card contains not only the password for the user login, but the authorization/access levels associated with the user. These access restrictions that are on the smart card are read by a smart card reader when the user logs in with the smart card. Although NTS does support the use of smart cards, NTS does not mention the use of access restrictions on the smart card for providing a known user access to a system, as recited in the claimed invention.

In view of the above, it is clear that NTS fails to disclose each and every limitation of claim 1. Therefore, amended independent claim 1 is patentable over NTS. Dependent claims 2, 5-9, and 11 are patentable for at least the same reasons. Further, independent claim 16 has been

amended to include similar allowable subject matter and is patentable over NTS for at least the same reasons as claim 1. Dependent claims 17, 19, and 20 are patentable for at least the same reasons as well. Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. § 103

Claims 3, 4, 12, 13, 15, 18, and 21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over NTS in view of NT File System Security and Auditing ("FSSA"). Independent claims 1, 15, and 16 have been amended by this reply to clarify the present invention as recited. To the extent that this rejection may still apply to the amended claims, this rejection is respectfully traversed.

As described above, NTS fails to disclose each and every limitation of the claimed invention. Further, FSSA fails to supply that which NTS lacks. In particular, FSSA relates to implementing audit policies and issues concerning NTFS and shared folders that give users centralized access to network files. FSSA discloses assigning share folder permissions for centralized access and securing network resource with NTFS permissions. FSSA fails to disclose or suggest that access restrictions are embedded onto a smart card such that when a user logs into a system using the smart card, the user is provided access to the system based on the access restrictions on the smart card itself. In fact, FSSA does not even discuss user access to a system using a smart card.

In view of the above, it is clear that amended independent claims 1, 15, and 16 are patentable over NTS and FSSA, whether considered separately or in combination. Further, dependent claims 3, 4, 12, 13, 18, and 21 are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claim 10 stand rejected under 35 U.S.C. 103(a) as being unpatentable over NTS in view of "Windows 2000 Advanced Documentation" ("Win2000"). To the extent that this rejection may still apply to the amended claims, this rejection is respectfully traversed.

As described above, NTS fails to disclose each and every limitation of the claimed invention. Further, Win2000 fails to supply that which NTS lacks. In particular, Win2000 discloses preparing a smart card certificate enrollment station. Win2000 informs a user how to

set up smart cards, smart card certificates, and install the necessary components. However, Win2000 fails to disclose or suggest that access restrictions are embedded onto a smart card such that when a user logs into a system using the smart card, the user is provided access to the system based on the access restrictions on the smart card itself.

In view of the above, it is clear that amended independent claim 1 is patentable over NTS and Win2000, whether considered separately or in combination. Further, dependent claim 10 is patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 03226/558001; P6570).

Dated: May 31, 2005   Respectfully submitted,

By _____
                                             Robert P. Lord
                                             Registration No.: 46,479
                                             Osha • Liang LLP
                                             1221 McKinney, Suite 2800
                                             Houston, Texas 77010
                                             (713) 228-8600
                                             (713) 228-8778 (Fax)
                                             Attorney for Applicant

95072_1.DOC
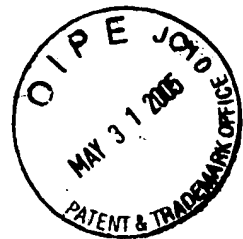
Application No. (if known): 09/895,530   Attorney Docket No.: 03226/558001; P6570

Certificate of Express Mailing Under 37 CFR 1.10

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Airbill No. EV703274175US in an envelope addressed to:

> Commissioner for Patents
> P.O. Box 1450
> Alexandria, VA 22313-1450

on _____May 31, 2005_____
                Date

_____
Signature

Yuki Tsukuda
Typed or printed name of person signing Certificate

_____   ____(713) 228-8600____
Registration Number, if applicable   Telephone Number

Note: Each paper must have its own certificate of mailing, or this certificate must identify
         each submitted paper.